

T S9/5/1

9/5/1

DIALOG(R) File 347:JAPIO

(c) 2004 JPO & JAPIO. All rts. reserv.

06124401 **Image available**

PORTABLE ELECTRONIC DEVICE AND ACCESS MANAGING METHOD FOR THE SAME

PUB. NO.: 11-065938 [JP 11065938 A]

PUBLISHED: March 09, 1999 (19990309)

INVENTOR(s): IIJIMA YASUO

APPLICANT(s): TOSHIBA CORP

APPL. NO.: 09-286930 [JP 97286930]

FILED: October 20, 1997 (19971020)

INTL CLASS: G06F-012/14; G06K-019/073

ABSTRACT

PROBLEM TO BE SOLVED: To provide a portable electronic device and an access managing method for the same with which certificate information different for each file can be used, access conditions can be changed for each file and each area and further the leak of certificate information can be prevented.

SOLUTION: Plural pieces of key data (password numbers) are stored in a data memory, these key data are collated with key data selectively inputted from the outside, and this collated result is stored for each piece of key data. In the case of access to the area of a data memory, when any one of the respective stored collated results is positive, access is enabled. When all the respective stored collated results are positive, access is enabled and it is set for each piece of instruction data for accessing the respective areas of the data memory.

COPYRIGHT: (C) 1999, JPO

?

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-65938

(43) 公開日 平成11年(1999) 3月9日

(51) Int.Cl.⁶

識別記号

F I

G 0 6 F 12/14

3 2 0

G 0 6 F 12/14

3 2 0 C

G 0 6 K 19/073

G 0 6 K 19/00

P

審査請求 有 請求項の数 7 O L (全 12 頁)

(21) 出願番号 特願平9-286930

(62) 分割の表示 特願昭63-211834の分割

(22) 出願日 昭和63年(1988) 8月26日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 飯島 康雄

神奈川県川崎市幸区柳町70番地 株式会社

東芝柳町工場内

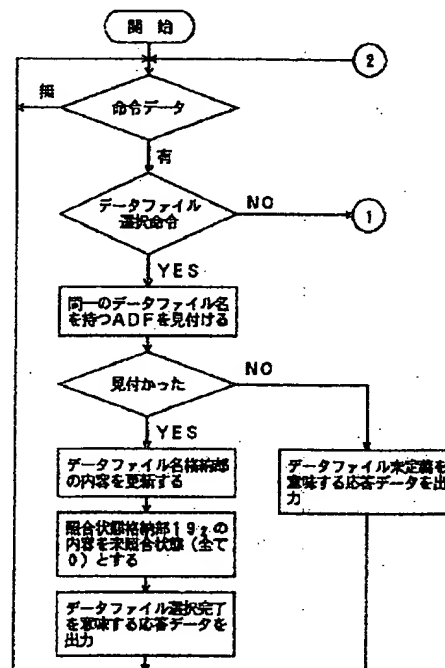
(74) 代理人 弁理士 鈴江 武彦 (外 6 名)

(54) 【発明の名称】 携帯可能電子装置および携帯可能電子装置におけるアクセス管理方法

(57) 【要約】

【課題】 ファイルごとに異なる認証情報を用いることができるとともに、ファイルごと、および、エリアごとにアクセス条件を変えることができ、しかも、認証情報の漏洩を防止することができる携帯可能電子装置および携帯可能電子装置におけるアクセス管理方法を提供する。

【解決手段】 データメモリ内に複数のキーデータ（暗証番号）を記憶しておき、これらキーデータを選択的に外部から入力されるキーデータと照合し、この照合結果を上記各キーデータごとに記憶しておき、データメモリのエリアに対してのアクセスの際、上記記憶してある各照合結果のうちいずれか1つが肯定的となっているときアクセス可能とし、上記記憶してある各照合結果の全てが肯定的となっているときアクセス可能とし、かつ、それらをデータメモリの各エリアに対するアクセスのための命令データごとに設定できるようにしている。



【特許請求の範囲】

【請求項1】 複数のファイルを有するメモリ部と、このメモリ部に対してアクセスを行なうための制御部を有し、選択的に外部とのデータの入出力を行なう携帯可能電子装置において、

前記各ファイルにはファイル名が付与されていて、各ファイルには複数のエリアと、ファイル内のエリアへのアクセスのために用いる複数の認証情報を記憶する認証情報記憶部が設けられており、かつ、各エリアには該エリアへのアクセスの際に必要な認証情報を示す照合状態確認情報およびこの照合状態確認情報にて示されている認証情報の組合わせをアンド論理とするかオア論理とするかの識別情報が記憶されており、

外部からファイル名を指定するファイル選択命令を受信した場合、前記各ファイルに付与されているファイル名に基づいてファイルを選択するファイル選択手段と、外部から認証情報の照合命令を受信した場合、前記選択手段にて選択されているファイル内に記憶されている認証情報と照合命令とともに外部から供給された認証情報とを照合する照合手段と、

この照合手段による照合の結果を前記複数の認証情報とともに保持する保持手段と、

前記複数のエリアへのアクセスの際に前記識別情報に基づき前記照合状態確認情報にて示されている認証情報の組合わせがアンド論理であるのかオア論理であるのかを判定する第1の判定手段と、

この第1の判定手段によりアンド論理であると判定された場合、前記照合状態確認情報にて示されている認証情報の全てについての照合結果が肯定的であるかを前記保持手段に保持されている照合結果に基づいて判定する第2の判定手段と、

この第2の判定手段によりオア論理であると判定された場合、前記照合状態確認情報にて示されている認証情報のうちいずれか1つが肯定的であるかを前記保持手段に保持されている照合結果に基づいて判定する第3の判定手段と、

前記第2の判定手段および前記第3の判定手段による判定結果が肯定的である場合に前記エリアへのアクセスを行なう手段と、

を具備したことを特徴とする携帯可能電子装置。

【請求項2】 前記複数のエリアには該エリアへのアクセスの際に必要な第1組の認証情報を示す第1の照合状態確認情報および該エリアへのアクセスの際に必要な第2組の認証情報を示す第2の照合状態確認情報が記憶されており、外部から受信した命令に基づき前記複数のエリアのうちいずれかにアクセスを行なう際に、前記第1の照合状態確認情報を用いるか前記第2の照合状態確認情報を用いるかを各命令データごとに対応して記憶している対応テーブルを有し、

エリアへのアクセスの際には受信した命令データと前記

対応テーブルとに基づき前記第1の照合状態確認情報を用いるか前記第2の照合状態確認情報を用いるかを選択する選択手段を具備したことを特徴とする請求項1記載の携帯可能電子装置。

【請求項3】 前記照合状態確認情報にて認証情報が示されておらず、かつ、前記識別情報がアンド論理の場合には前記照合結果を判定することなく、エリアへのアクセスを不可とするアクセス禁止手段と、

前記照合状態確認情報にて認証情報が示されておらず、かつ、前記識別情報がオア論理の場合には前記照合結果を参照することなく、エリアへのアクセスを許可するアクセス許可手段と、

を具備したことを特徴とする請求項1記載の携帯可能電子装置。

【請求項4】 前記携帯可能電子装置は前記メモリ部を構成するデータメモリと前記制御部を構成する制御素子およびプログラムメモリとからなる1つのICチップにより構成されていることを特徴とする請求項1記載の携帯可能電子装置。

【請求項5】 複数のファイルを有するメモリ部と、このメモリ部に対してアクセスを行なうための制御部を有し、選択的に外部とのデータの入出力を行なう携帯可能電子装置におけるアクセス管理方法において、前記各ファイルにはファイル名が付与されていて、各ファイルには複数のエリアを設けるとともに、ファイル内のエリアへのアクセスのために用いる複数の認証情報を記憶し、かつ、各エリアには該エリアへのアクセスの際に必要な認証情報を示す照合状態確認情報およびこの照合状態確認情報にて示されている認証情報の組合わせをアンド論理とするかオア論理とするかの識別情報を記憶しておき、

外部からファイル名を指定するファイル選択命令を受信した場合、前記各ファイルに付与されているファイル名に基づいてファイルを選択し、

外部から認証情報の照合命令を受信した場合、前記選択されているファイル内に記憶されている認証情報と照合命令とともに外部から供給された認証情報とを照合し、この照合の結果を前記複数の認証情報ごとに対応しておき、

前記複数のエリアへのアクセスの際に前記識別情報に基づき前記照合状態確認情報にて示されている認証情報の組合わせがアンド論理であるのかオア論理であるのかを判定する第1の判定ステップと、

この第1の判定ステップによりアンド論理であると判定された場合、前記照合状態確認情報にて示されている認証情報の全てについての照合結果が肯定的であるかを前記保持されている照合結果に基づいて判定する第2の判定ステップと、

前記第1の判定ステップによりオア論理であると判定された場合、前記照合状態確認情報にて示されている認証

情報のうちいずれか1つが肯定的であるかを前記保持されている照合結果に基づいて判定する第3の判定ステップと、

前記第2の判定ステップおよび前記第3の判定ステップによる判定結果が肯定的である場合に前記エリアへのアクセスを行なうステップと、

を具備したことを特徴とする携帯可能電子装置におけるアクセス管理方法。

【請求項6】前記複数のエリアには該エリアへのアクセスの際に必要な第1組の認証情報を示す第1の照合状態確認情報および該エリアへのアクセスの際に必要な第2組の認証情報を示す第2の照合状態確認情報が記憶されており、外部から受信した命令に基づき前記複数のエリアのうちいずれかにアクセスを行なう際に、前記第1の照合状態確認情報を用いるか前記第2の照合状態確認情報を用いるかを各命令データとに対応して記憶している対応テーブルを有し、

エリアへのアクセスの際には受信した命令データと前記対応テーブルに基づき前記第1の照合状態確認情報を用いるか前記第2の照合状態確認情報を用いるかを選択する選択ステップを具備したことを特徴とする請求項5記載の携帯可能電子装置におけるアクセス管理方法。

【請求項7】前記照合状態確認情報にて認証情報が示されておらず、かつ、前記識別情報がアンド論理の場合には前記照合結果を判定することなく、エリアへのアクセスを不可とし、前記照合状態確認情報にて認証情報が示されておらず、かつ、前記識別情報がオア論理の場合には前記照合結果を参照することなく、エリアへのアクセスを許可するようにしたことを特徴とする請求項5記載の携帯可能電子装置におけるアクセス管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、たとえば、不揮発性メモリおよびCPUなどの制御素子を有するIC（集積回路）チップを内蔵した、いわゆるICカードと称される携帯可能電子装置、および、この携帯可能電子装置におけるアクセス管理方法に関する。

【0002】

【従来の技術】近年、新たな携帯可能なデータ記憶媒体として、消去可能な不揮発性メモリおよびCPUなどの制御素子を有するICチップを内蔵した、いわゆるICカードが開発されている。

【0003】この種のICカードは、内蔵するメモリに認証情報としての暗証番号が記憶されており、外部から暗証番号を入力することにより、メモリに記憶されている登録暗証番号とを内部で照合し、その照合結果に応じて以降のメモリのエリアに対するアクセスの可否を決定するようになっている。

【0004】

【発明が解決しようとする課題】さて、ICカードの多

目的利用のためには、メモリ内に複数の暗証番号を記憶しておくことにより、メモリのエリアへのアクセスに必要な暗証番号の種々の組合せをエリアごとに設定でき、かつ、エリアへのアクセスとして、たとえば、読出し、書込みなどの命令データごとにも設定すれば、ICカードシステムの構築において柔軟性が得られる。しかし、従来のICカードではそれが不可能であった。このため、エリアへのアクセス条件がきめ細かく設定できず、ICカードシステムの構築において柔軟性に欠けるという欠点があった。

【0005】また、エリアに対するアクセスの可否を決定する方法として、メモリ内に複数の暗証番号を記憶しておくとともに、各エリアに対しどの暗証番号が照合されるとアクセス可能なのかを示す識別情報を各エリアごとに対応させて記憶しておくことにより、アクセスのたびに暗証番号の照合結果と上記識別情報とを比較してアクセスの可否を決定することが考えられる。しかし、上記識別情報が全てのアクセス命令データに共通に使用されるとしたら、全ての命令データに対するアクセス条件が同一となり、運用しにくくなる。

【0006】そこで、本発明は、ファイルごとに異なる認証情報を用いることができるとともに、ファイルごと、および、エリアごとにアクセス条件を変えることができ、しかも、認証情報の漏洩を防止することができる携帯可能電子装置および携帯可能電子装置におけるアクセス管理方法を提供することを目的とする。

【0007】

【課題を解決するための手段】本発明の携帯可能電子装置は、複数のファイルを有するメモリ部と、このメモリ部に対してアクセスを行なうための制御部を有し、選択的に外部とのデータの入出力を行なう携帯可能電子装置において、前記各ファイルにはファイル名が付与されていて、各ファイルには複数のエリアと、ファイル内のエリアへのアクセスのために用いる複数の認証情報を記憶する認証情報記憶部が設けられており、かつ、各エリアには該エリアへのアクセスの際に必要な認証情報を示す照合状態確認情報およびこの照合状態確認情報にて示されている認証情報の組合せをアンド論理とするかオア論理とするかの識別情報が記憶されており、外部からファイル名を指定するファイル選択命令を受信した場合、前記各ファイルに付与されているファイル名に基づいてファイルを選択するファイル選択手段と、外部から認証情報の照合命令を受信した場合、前記選択手段にて選択されているファイル内に記憶されている認証情報と照合命令とともに外部から供給された認証情報とを照合する照合手段と、この照合手段による照合の結果を前記複数の認証情報ごとに保持する保持手段と、前記複数のエリアへのアクセスの際に前記識別情報に基づき前記照合状態確認情報にて示されている認証情報の組合せがアンド論理であるのかオア論理であるのかを判定する第1の

判定手段と、この第1の判定手段によりアンド論理であると判定された場合、前記照合状態確認情報にて示されている認証情報の全てについての照合結果が肯定的であるかを前記保持手段に保持されている照合結果に基づいて判定する第2の判定手段と、この第2の判定手段によりオア論理であると判定された場合、前記照合状態確認情報にて示されている認証情報のうちいずれか1つが肯定的であるかを前記保持手段に保持されている照合結果に基づいて判定する第3の判定手段と、前記第2の判定手段および前記第3の判定手段による判定結果が肯定的である場合に前記エリアへのアクセスを行なう手段とを具備したことを特徴とする。

【0008】また、本発明の携帯可能電子装置におけるアクセス管理方法は、複数のファイルを有するメモリ部と、このメモリ部に対してアクセスを行なうための制御部を有し、選択的に外部とのデータの入出力を行なう携帯可能電子装置におけるアクセス管理方法において、前記各ファイルにはファイル名が付与されていて、各ファイルには複数のエリアを設けるとともに、ファイル内のエリアへのアクセスのために用いる複数の認証情報を記憶し、かつ、各エリアには該エリアへのアクセスの際に必要な認証情報を示す照合状態確認情報およびこの照合状態確認情報にて示されている認証情報の組合せをアンド論理とするかオア論理とするかの識別情報を記憶しておき、外部からファイル名を指定するファイル選択命令を受信した場合、前記各ファイルに付与されているファイル名に基づいてファイルを選択し、外部から認証情報の照合命令を受信した場合、前記選択されているファイル内に記憶されている認証情報と照合命令とともに外部から供給された認証情報とを照合し、この照合の結果を前記複数の認証情報ごとに保持しておき、前記複数のエリアへのアクセスの際に前記識別情報に基づき前記情報照合状態確認情報にて示されている認証情報の組合せがアンド論理であるのかオア論理であるのかを判定する第1の判定ステップと、この第1の判定ステップによりアンド論理であると判定された場合、前記照合状態確認情報にて示されている認証情報の全てについての照合結果が肯定的であるかを前記保持されている照合結果に基づいて判定する第2の判定ステップと、前記第1の判定ステップによりオア論理であると判定された場合、前記照合状態確認情報にて示されている認証情報のうちいずれか1つが肯定的であるかを前記保持されている照合結果に基づいて判定する第3の判定ステップと、前記第2の判定ステップおよび前記第3の判定ステップによる判定結果が肯定的である場合に前記エリアへのアクセスを行なうステップとを具備したことを特徴とする。

【0009】本発明によれば、内部に複数の認証情報を記憶しておき、これら認証情報を選択的に外部から入力される認証情報と照合し、この照合結果を上記各認証情報ごとに記憶しておき、エリアに対してのアクセスの

際、上記記憶してある各照合結果のうちいずれか1つが肯定的となっているときアクセス可能とし、上記記憶してある各照合結果の全てが肯定的となっているときアクセス可能とするものである。

【0010】これにより、各エリアごとにエリアへのアクセスに必要な認証情報の組合せを任意に設定でき、しかも、その組合せに対して特にアンド論理あるいはオア論理を合せて設定できる。したがって、各エリアへのアクセス条件がきめ細かく設定でき、システム構築において柔軟性が得られるようになる。

【0011】すなわち、本発明によれば、ファイルごとに認証情報が記憶されているので、ファイルごとに異なる認証情報を用いることができる。また、ファイルごとの認証情報を用いてファイル内の各エリアのアクセス条件が記憶されているので、ファイルごと、および、エリアごとにアクセス条件を変えることができる。さらに、ファイルを選択していないと認証情報の照合が不可能となるので、認証情報の漏洩を防止することができる。

【0012】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。図14は、本発明に係る携帯可能電子装置としてのICカードを取扱う端末装置の構成例を示すものである。すなわち、この端末装置は、ICカード1をカードリーダー・ライター2を介してCPUなどからなる制御部3と接続可能にするとともに、制御部3にキーボード4、CRTディスプレイ装置5、プリンタ6、および、フロッピーディスク装置7を接続して構成される。

【0013】ICカード1は、ユーザが保持し、たとえば、商品購入などの際にユーザのみが知得している暗証番号の参照や必要データの蓄積などを行なうもので、たとえば、図13にその機能ブロックを示すように、リード・ライト部11、暗証設定・暗証照合部12、および、暗号化・復号化部13などの基本機能を実行する部分と、これらの基本機能を管理するスーパーバイザ14とで構成されている。

【0014】リード・ライト部11は、データメモリ16などに対してデータの読出し、書込み、あるいは消去を行なう機能である。暗証設定・暗証照合部12は、ユーザが設定した暗証番号の記憶および読出禁止処理を行なうとともに、暗証番号の設定後にその暗証番号の照合を行ない、以後の処理の許可を与える機能である。

【0015】暗号化・復号化部13は、たとえば、通信回線を介して制御部3から他の端末装置へデータを送信する場合の通信データの漏洩、偽造を防止するための暗号化や、暗号化されたデータの復号化を行なうものであり、たとえば、DES(Data Encryption Standard)など、充分な暗号強度を有する暗号化アルゴリズムにしたがってデータ処理を行なう機能である。

【0016】スーパーバイザ14は、カードリーダー・ライタ2から入力された機能コード、もしくは、データの付加された機能コードを解釈し、前記基本機能のうち必要な機能を選択して実行させる機能である。

【0017】これらの諸機能を発揮させるために、ICカード1は、たとえば、図12に示すように、CPUなどの制御素子(制御部)15、メモリ部としてのデータメモリ16、プログラムメモリ17、および、カードリーダー・ライタ2との電気的接触を得るためのコンタクト部18によって構成されており、これらのうち制御素子15、データメモリ16、および、プログラムメモリ17は1つのICチップ(あるいは複数のICチップ)で構成されてICカード本体内に埋設されている。

【0018】プログラムメモリ17は、たとえば、マスクROMで構成されており、前記各基本機能を実現するサブルーチンを備えた制御素子15の制御プログラムなどを記憶するものである。

【0019】データメモリ16は、各種データの記憶に使用され、たとえば、EEPROMなどの消去可能な不揮発性メモリで構成されている。そして、データメモリ16は、たとえば、図4に示すように、全てのアプリケーションで運用する1つのコモンデータファイル21と、アプリケーション個別に運用する複数(図では2つの)のアプリケーションデータファイル221、222とによって構成されており、それぞれのデータファイル21、221、222には、複数の認証情報としてのキーデータ(暗証番号)が記憶されているとともに、複数のエリアが存在している。

【0020】アプリケーションデータファイル221、222には、それぞれデータファイル名(DFN)が付与されており、後述するデータファイル選択命令データを用いて、このデータファイル名を指定することにより、以降のアクセス対象となるアプリケーションデータファイルを認識するようになっている。

【0021】各キーデータには、たとえば、図5に示すように、キーデータを指定する識別情報(KID)が付与されており、後述するキーデータ照合命令データを用いて、この識別情報を指定することにより、照合処理の対象となるキーデータを認識するようになっている。

【0022】図4の例では、コモンデータファイル21に属するキーデータ1、2、3に対して、それぞれKID01、KID02、KID03が付与されている。また、アプリケーションデータファイル221に属するキーデータX4、X5、X6に対して、それぞれKID04、KID05、KID06が付与されている。さらに、アプリケーションデータファイル222に属するキーデータY4、Y5、Y6に対しても、それぞれKID04、KID05、KID06が付与されている。

【0023】また、各キーデータには、たとえば、図5に示すように、個別に照合状態指定情報が付与されてお

り、以降のアクセスに必要なキーデータが照合済となっているか否かの識別に使用される。

【0024】キーデータが照合済であるか否かの情報は、図7に示す照合状態格納部231、232に格納される。この照合状態格納部231、232は、たとえば、制御素子15に内蔵されたRAM内に設けられており、コモンデータファイル21に属するキーデータの場合には照合状態格納部231に、また、アプリケーションデータファイル221、222に属するキーデータの場合には照合状態格納部232に、それぞれ格納される。

【0025】また、図7に示すように、照合状態格納部231、232とともにデータファイル名格納部24が設けられており、このデータファイル名格納部24には、後述するデータファイル選択命令データによりアクセス対象として選択されたデータファイルのデータファイル名が格納される。

【0026】一方、各エリアには、たとえば、図6に示すように、エリアを指定する識別情報(AID)が付与されており、後述するエリア処理命令データを用いて、この識別情報を指定することにより、エリア処理の対象となるエリアを認識するようになっている。

【0027】図4の例では、コモンデータファイル21に属するエリアG、Hに対して、それぞれAIDgg、AIDhhが付与されている。また、アプリケーションデータファイル221に属するエリアA、B、Cに対して、それぞれAIDaa、AIDbb、AIDccが付与されている。さらに、アプリケーションデータファイル222に属するエリアD、E、Fに対して、それぞれAIDdd、AIDee、AIDffが付与されている。

【0028】また、各エリアには、たとえば、図6に示すように、個別に第1、第2照合状態確認情報が付与されているとともに、これら第1、第2照合状態確認情報にはそれぞれ論理情報(AまたはO)が付与されている。第1、第2照合状態確認情報は、エリアアクセスの際に必要なキーデータの照合状態を要求するものである。また、論理情報は、照合状態確認情報の組合せをアンド(AND)論理とするかオア(OR)論理とするかという識別情報であり、アンド論理の場合は「A」、オア論理の場合は「O」となっている。

【0029】図8は、各エリアに割当てられた2つの照合状態確認情報を命令コード別に選択するためのデータテーブルを示すもので、各種命令コードにそれぞれ対応して照合状態確認情報を選択するための選択情報が格納されており、このデータテーブルは、たとえば、データメモリ16内に設けられている。

【0030】次に、このような構成において、図1ないし図3に示すフローチャートを参照しつつ動作を説明する。なお、フローチャート上では、コモンデータファイル21をCDF、アプリケーションデータファイル22

10

20

30

40

50

1, 222をADFと略記する。

【0031】まず、データファイルの選択処理を説明する。定常状態においては、命令データ待ち状態になっており、この状態で命令データが入力されると、制御素子15は、図9に示すようなデータファイル選択命令データか否かを判断する。この判断の結果、データファイル選択命令データでなければ、制御素子15は別の処理を行なう。

【0032】上記命令データの判断の結果、データファイル選択命令データであれば、制御素子15は、データメモリ16から本命令データ中のデータファイル名と同一のデータファイル名を持つアプリケーションデータファイルを見付ける。もし見付からなければ、制御素子15は、データファイル未定義を意味する応答データを出力し、命令データ待ち状態に戻る。

【0033】もし見付かれれば、制御素子15は、図7のデータファイル名格納部24に本命令データ中のデータファイル名を格納し、かつ、照合状態格納部232の内容を未照合状態、すなわち、全てのビットを「0」とする。そして、制御素子15は、データファイル選択完了を意味する応答データを出力し、命令データ待ち状態に戻る。

【0034】ICカードの起動時には、図7の各格納部231, 232, 24の内容は全て「0」となっており、このとき、たとえば、データファイル名「XXX」を有するデータファイル選択命令データが入力されると、データファイル名格納部24には「XXX」という値が格納される。

【0035】次に、キーデータの照合処理を説明する。前記データファイル選択命令データか否かの判断の結果、データファイル選択命令データでなければ、制御素子15は、次に図10に示すようなキーデータ照合命令データか否かを判断する。この判断の結果、キーデータ照合命令データでなければ、制御素子15は別の処理を行なう。

【0036】上記命令データの判断の結果、キーデータ照合命令データであれば、制御素子15は、まず、データファイル名格納部24の内容が「0」となっているか否か（データファイルが選択されているか否か）を判断する。この判断の結果、もし「0」となっていれば、データファイルが何も選択されていないことになる。したがって、制御素子15は、コモンデータファイル21を参照することにより、本命令データ中の識別情報(KID)と同一の識別情報(KID)を持つキーデータを見付ける。

【0037】上記判断の結果、もし「0」となっていなければ、データファイルが選択されていることになる。したがって、制御素子15は、コモンデータファイル21、および、選択されたアプリケーションデータファイル221または222を参照することにより、同様に本

命令データ中の識別情報と同一の識別情報を持つキーデータを見付ける。もし見付からなければ、制御素子15は、キーデータ未定義を意味する応答データを出力し、命令データ待ち状態に戻る。

【0038】もし見付かれれば、制御素子15は、そのキーデータと本命令データ中のキーデータとを照合する。この照合の結果、両者が一致していれば、制御素子15は、このキーデータがコモンデータファイル21に属するか、アプリケーションデータファイル221, 222に属するかを判断する。

【0039】この判断の結果、コモンデータファイル21に属するものであれば、制御素子15は、そのキーデータに付与されている照合状態指定情報を参照し、「1」となっているビットと同一の照合状態格納部231のビットを「1」にする。

【0040】また、アプリケーションデータファイル221, 222に属するものであれば、制御素子15は、同様に、こんどは照合状態格納部232の同一ビットを「1」にする。そして、キーデータ一致を意味する応答データを出力し、命令データ待ち状態に戻る。

【0041】上記キーデータの照合の結果、両者が一致していなければ、制御素子15は、同様にして、照合状態格納部231あるいは照合状態格納部232の同一ビットを「0」にする。そして、キーデータ不一致を意味する応答データを出力し、命令データ待ち状態に戻る。

【0042】たとえば、データファイル選択命令データによりアプリケーションデータファイル222を選択した後、キーデータI、キーデータY5およびY6を照合すると、照合状態格納部231の内容は「10000000」、照合状態格納部232の内容は「00001100」、また、データファイル名格納部24の内容は「YYY」となる。この後に、アプリケーションデータファイル221を選択すると、照合状態格納部231の内容は変化せず、照合状態格納部232の内容は「00000000」となり、また、データファイル名格納部24の内容は「XXX」となる。

【0043】次に、エリア処理（エリア内データの読出、書込、消去）を説明する。前記キーデータ照合命令データか否かの判断の結果、キーデータ照合命令データでなければ、制御素子15は、次に図11(a)に示すような読出命令データ、図11(b)に示すような書込命令データ、あるいは、図11(c)に示すような消去命令データか否かを判断する。この判断の結果、図11のようなエリア処理命令データでなければ、制御素子15は別の処理を行なう。

【0044】上記命令データの判断の結果、エリア処理命令データであれば、制御素子15は、まず、データファイル名格納部24の内容が「0」となっているか否かを判断する。この判断の結果、もし「0」となっていれば、データファイルが何も選択されていないことにな

る。したがって、制御素子15は、コモンデータファイル21を参照することにより、本命令データ中の識別情報(AID)と同一の識別情報(AID)を持つエリアを見付ける。

【0045】上記判断の結果、もし「0」となっていないければ、データファイルが選択されていることになる。したがって、制御素子15は、コモンデータファイル21、および、選択されたアプリケーションデータファイル221または222を参照することにより、同様に本命令データ中の識別情報と同一の識別情報を持つエリアを見付ける。もし見付からなければ、制御素子15は、

エリア未定義を意味する応答データを出力し、命令データ待ち状態に戻る。

【0046】もし見付かれれば、制御素子15は、照合状態格納部231の内容と照合状態格納部232の内容との論理和をとり、その結果を「結果1」としておく。次に、制御素子15は、本命令データ中の命令コードと同一の命令コードを図8のデータテーブルから検索することにより、各エリアに割当てられている2つの照合状態確認情報を選択する。たとえば、エリア処理命令データが読出命令データであれば、その命令コードが「zz」なので、それに対応する選択情報「1」により第1照合状態確認情報が選択され、書込命令データであれば、その命令コードが「ww」なので、それに対応する選択情報「2」により第2照合状態確認情報が選択され、消去命令データであれば、その命令コードが「vv」なので、それに対応する選択情報「2」により第2照合状態確認情報が選択される。

【0047】このようにして、第1または第2照合状態確認情報を選択すると、制御素子15は、その選択した照合状態確認情報を参照し、それに付与されている論理情報がアンド論理となっているか否かを判断する。この判断の結果、もしアンド論理でなければ(オア論理となっている)、制御素子15は、照合状態確認情報の全てのビットが「0」か否かを判断する。この判断の結果、もし全てのビットが「0」であれば、制御素子15は、照合状態を確認せずにエリアに対する処理を行なう。

【0048】上記判断の結果、もしどれかのビットが「1」となっていれば、制御素子15は、その「1」となっているビットに対応する前記結果1内のビットのどれかが「1」となっているか否かを判断する。この判断の結果、もしどのビットも「1」となっていないければ、制御素子15は、アクセス不可を意味する応答データを出力し、命令データ待ち状態に戻る。上記判断の結果、もしどれか1つのビットでも「1」となっていれば、制御素子15は、エリアに対する処理を行なう。

【0049】上記論理情報の判断の結果、もしアンド論理になっていければ、制御素子15は、同様に照合状態確認情報の全てのビットが「0」か否かを判断する。この判断の結果、もし全てのビットが「0」であれば、制御

素子15は、エリアへのアクセスが禁止されていると判断して、アクセス不可を意味する応答データを出力し、命令データ待ち状態に戻る。

【0050】上記判断の結果、もしどれかのビットが「1」となっていれば、制御素子15は、本照合状態確認情報と前記結果1とを比較する。この比較の結果、もし両者が一致していなければ、制御素子15は、同様にアクセス不可を意味する応答データを出力し、命令データ待ち状態に戻る。上記比較の結果、もし両者が一致していれば、制御素子15は、エリアに対する処理を行ない、その処理終了後、処理結果を応答データとして出力し、命令データ待ち状態に戻る。

【0051】ここで、具体的に説明すると、図4の例において、たとえば、エリアBについては、それに付与されている第1照合状態確認情報の論理情報がアンド論理(A)で、第1照合状態確認情報は「10000000」となっている。したがって、キーデータ1の照合のみが済んでいる状態でエリアBへの読出しアクセスが可能となる。また、第2照合状態確認情報は「00000000」で、その論理情報がオア論理(O)となっている。したがって、エリアBへの書込みおよび消去アクセスは、キーデータの照合が不要であることを示している。

【0052】また、エリアCについては、第1照合状態確認情報は「00000000」で、その論理情報がアンド論理(A)となっている。したがって、エリアCへの読出しアクセスは不可となる。また、第2照合状態確認情報は「00001100」で、その論理情報がオア論理(O)となっている。したがって、キーデータX5あるいはキーデータX6のどちらかの照合が済んでいければ、エリアCへの書込みおよび消去アクセスは可能となる。

【0053】また、キーデータY5およびキーデータY6の照合後、アプリケーションデータファイル221を選択してエリアCへの書込みアクセスを実行すると、その選択時にキーデータY5およびキーデータY6の照合状態はクリアされるため、アクセスは不可となる。

【0054】すなわち、このことから、アプリケーションデータファイル221、222内のキーデータの照合状態は、同一のアプリケーションデータファイル内のエリアへのアクセスに対してのみ有効となる。

【0055】また、アプリケーションデータファイル221のキーデータX4とアプリケーションデータファイル222のキーデータY4とは同一の識別情報(KID)を与えられているが、識別情報の指定の際には、どちらか1つのアプリケーションデータファイルのみがアクセスの対象となっているため、混同することはない。ただし、コモンデータファイルと他のアプリケーションデータファイルの間では同一の識別情報(KID)を使用しないようにする。なお、エリアに対して与える識

別情報(AID)についても同様である。

【0056】また、同一のアプリケーションデータファイル内において、識別情報(AID)および識別情報(KID)については、命令データとしてどちらに対してアクセスするかが一義的に決まるため、同一の値を使用してもよい。

【0057】さらに、各エリアに対して与えられる照合状態確認情報の数についても、エリアに対する命令および処理の数に対応して変更可能である。このように、データメモリ内に複数のキーデータ(暗証番号)を記憶しておき、これらキーデータを選択的に外部から入力されるキーデータと照合し、この照合結果を上記各キーデータごとに記憶しておき、データメモリのエリアに対してのアクセスの際、上記記憶してある各照合結果のうちいずれか1つが肯定的となっているときアクセス可能とし、上記記憶してある各照合結果の全てが肯定的となっているときアクセス可能とし、かつ、それらをデータメモリの各エリアに対するアクセスのための命令データごとに設定できるようにしている。

【0058】これにより、データメモリの各エリアごとにエリアへのアクセスに必要なとなるキーデータの組合せを任意に設定でき、その組合せに対して特にアンド論理あるいはオア論理を合せて設定でき、かつ、その組合せはデータメモリの各エリアに対するアクセスのための命令データごとに設定できる。したがって、データメモリの各エリアへのアクセス条件がきめ細かく設定でき、ICカードシステムの構築において柔軟性が得られるようになる。

【0059】すなわち、ファイルごとにキーデータ(暗証番号)が記憶されているので、ファイルごとに異なるキーデータを用いることができる。また、ファイルごとのキーデータを用いてファイル内の各エリアのアクセス条件が記憶されているので、ファイルごと、および、エリアごとにアクセス条件を変えることができる。さらに、ファイルを選択していないとキーデータの照合が不可能となるので、キーデータの漏洩を防止することができ*

きる。

【0060】

【発明の効果】以上詳述したように本発明によれば、ファイルごとに異なる認証情報を用いることができるとともに、ファイルごと、および、エリアごとにアクセス条件を変えることができ、しかも、認証情報の漏洩を防止することができる携帯可能電子装置および携帯可能電子装置におけるアクセス管理方法を提供できる。

【図面の簡単な説明】

【図1】各処理動作を説明するフローチャート。

【図2】各処理動作を説明するフローチャート。

【図3】各処理動作を説明するフローチャート。

【図4】データメモリのファイル構造を示す図。

【図5】キーデータに対する諸情報を説明する図。

【図6】エリアに対する諸情報を説明する図。

【図7】照合状態格納部およびデータファイル名格納部を説明する図。

【図8】各種命令コードに対応して照合状態確認情報を選択するための選択情報が格納されているデータテーブルを説明する図。

【図9】データファイル選択命令データのフォーマット例を示す図。

【図10】キーデータ照合命令データのフォーマット例を示す図。

【図11】エリアへの読出命令データ、書込命令データ、および、消去命令データのフォーマット例を示す図。

【図12】ICカードの構成を示すブロック図。

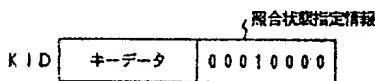
【図13】ICカードの機能ブロックを示す図。

【図14】端末装置の構成を示すブロック図。

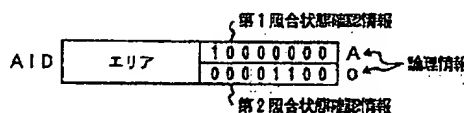
【符号の説明】

1……ICカード(携帯可能電子装置)、15……制御素子(制御部)、16……データメモリ(メモリ部)、17……プログラムメモリ、21……コモンデータファイル、221、222……アプリケーションデータファイル、231、232……照合状態格納部。

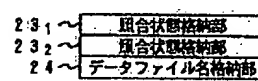
【図5】



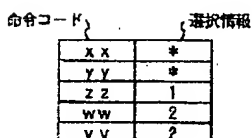
【図6】



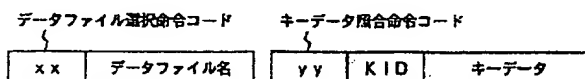
【図7】



【図8】

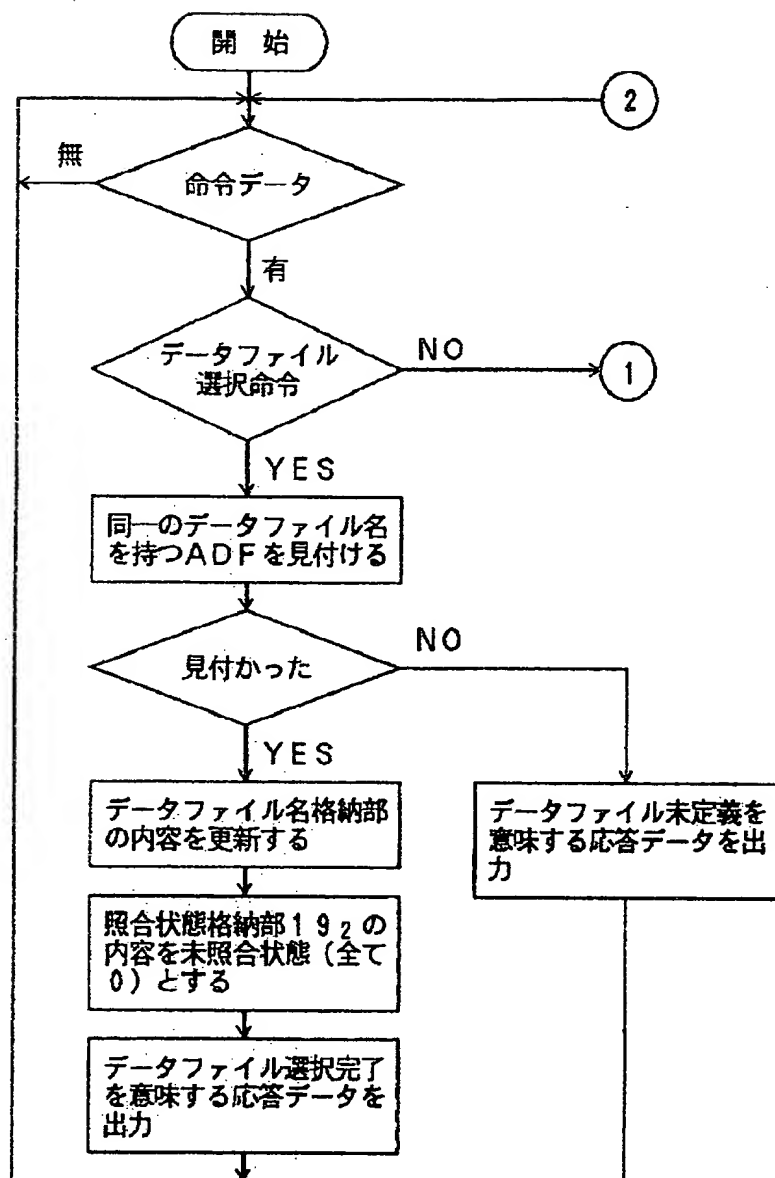


【図9】

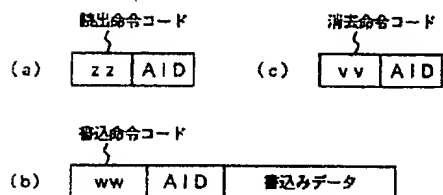


【図10】

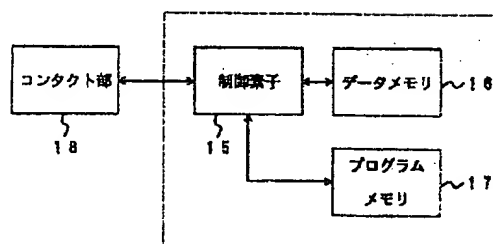
【図1】



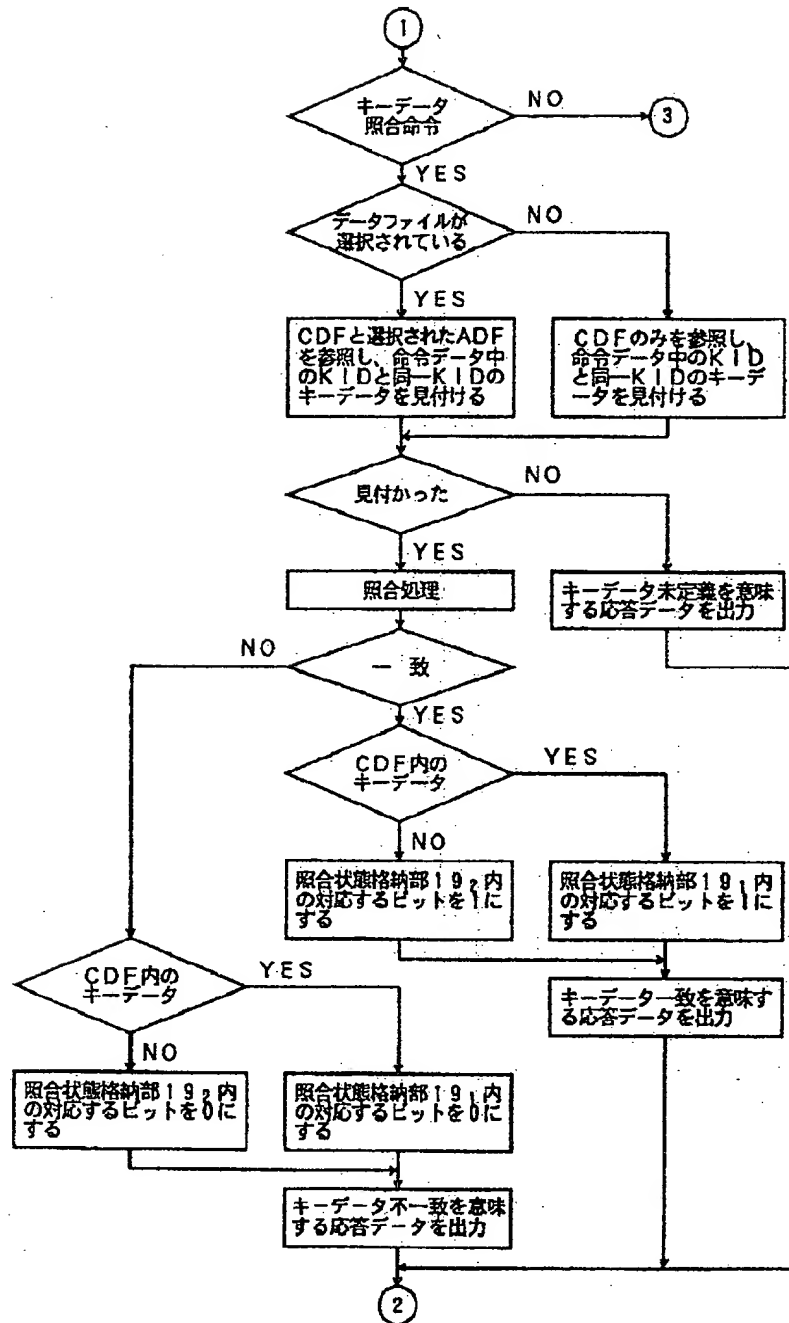
【図11】



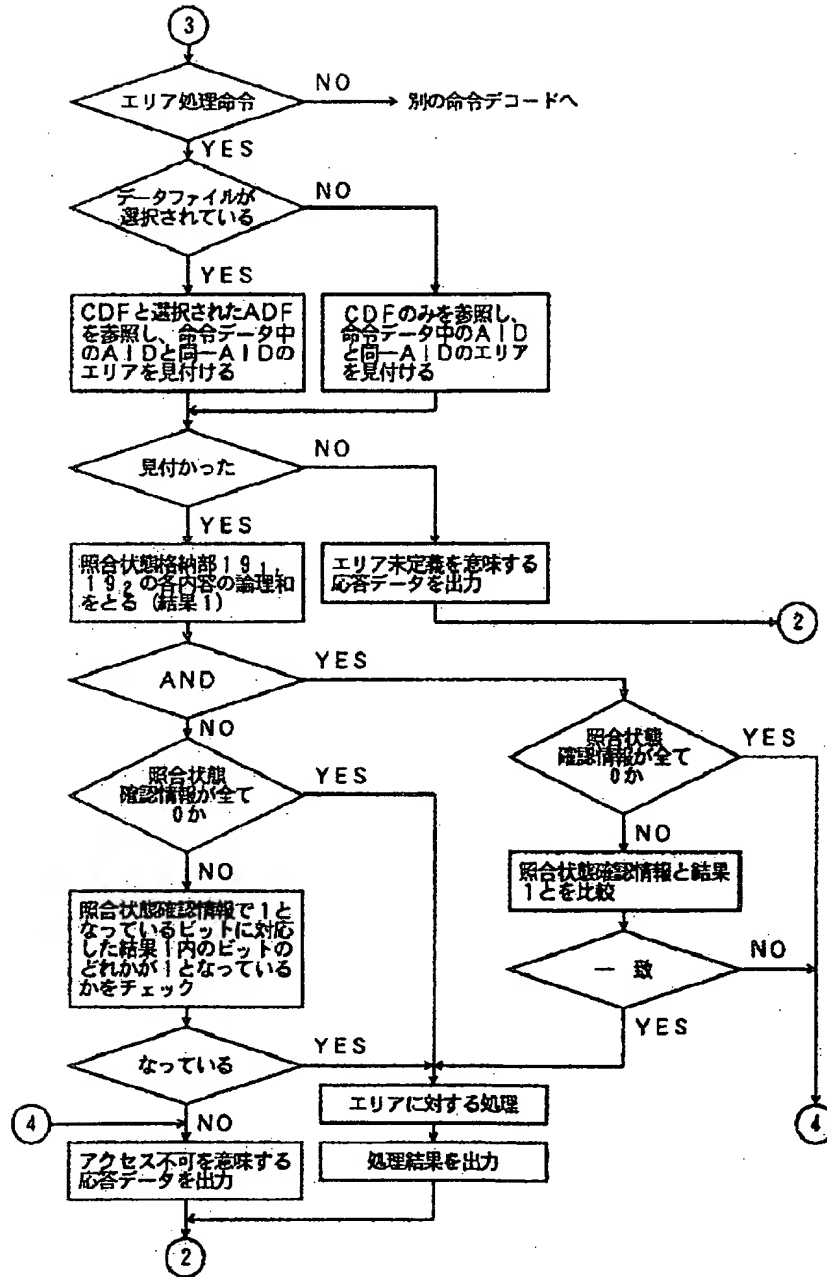
【図12】



【図2】



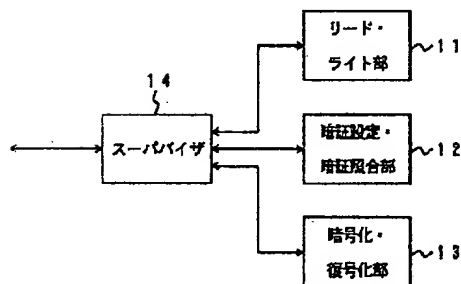
【図3】



【図4】

21~		KID01	キーデータ1	10000000	AIDgg	エリアG	10000000	A
		KID02	キーデータ2	01000000	AIDhh	エリアH	10001000	A
		KID03	キーデータ3	00100000			01000000	A
DFN=XXX		KID04	キーデータX4	00010000	AIDaa	エリアA	10000000	A
		KID05	キーデータX5	00001000	AIDbb	エリアB	10000000	A
		KID06	キーデータX6	00000100	AIDcc	エリアC	00000000	A
22~		KID04	キーデータY4	00010000	AIDdd	エリアD	10000000	A
		KID05	キーデータY5	00001000	AIDee	エリアE	10000000	A
		KID06	キーデータY6	00000010	AIDff	エリアF	00000000	A

【図13】



【図14】

